REMARKS

I. Amendments to the Claims

Applicant amends claims 26 and 50. The amendments are supported by Applicant's specification at, for example, page 5, lines 16-20, and page 6, lines 19-24. Claims 26-50 are pending and under examination.

II. Final Office Action

In the Final Office Action, the Examiner took the following actions:

(1) objected to the specification;

(2) rejected claims 26-37 and 50 under 35 U.S.C. § 101 as allegedly being directed to non-statutory subject matter;

(3) rejected claims 26-28, 30-32, 35-40[1], 42-44, and 47-50 under 35 U.S.C. § 102(a) as being anticipated by European Publication No. EP 1330095 A1 ("Lahtinen");

(4) rejected claims 29 and 41 under 35 U.S.C. § 103(a) as being unpatentable over Lahtinen in view of U.S. Patent Application Pub. No. 2003/0149888 A1 ("Yadav"); and

(5) rejected claims 33, 34, 45, and 46 under 35 U.S.C. § 103(a) as being unpatentable over Lahtinen in view of U.S. Patent Application Pub. No. 2002/0105910 ("Maher").

III. Response to Objection and Rejections

Applicant respectfully traverses the aforementioned objection and rejections, and requests reconsideration based on the following remarks.

A. Objection to the Specification

The Final Office Action, on page 3, objected to Applicant's specification for allegedly failing to provide antecedent basis for the claimed limitations "sniffer, implemented using the one or more computers," "a pattern matching engine, implemented using the one or more

[1] The Final Office Action, under item 13 on page 5, listed claim 41 and not claim 40 under this rejection; however, in the ensuing explanation, the Office Action instead rejected claim 40 and not claim 41.

computers," and "a response analysis engine, implemented using the one or more computers," as previously recited in claim 26. While not agreeing with the rejection, Applicant amends claim 26 as indicated above, to overcome this objection. The amendments are supported by Applicant's specification at, for example, page 5, lines 16-20, and page 6, lines 19-24. Accordingly, Applicant respectfully requests withdrawal of the objection.

B. Claim Rejections under 35 U.S.C. § 101

The Final Office Action, on pages 3-4, rejected claims 26-37 under 35 U.S.C. § 101 due to the recitation of "a sniffer," "a pattern matching engine," and "a response analysis engine," in claim 26. While not agreeing with the rejection, Applicant amends claim 26 to recite that the intrusion detection system comprises "at least one computer; and a non-transitory computer readable medium encoded with a computer program product loadable into a memory of the at least one computer, the computer program product including: instructions for a sniffer ... instructions for a pattern matching engine [and] instructions for a response analysis engine."

Further, on page 4, the Final Office Action rejected claim 50, alleging that "it appears that the 'computer readable medium encoded with a computer program product' [as recited in claim 50,] may embody signals and carrier waves."

Without conceding to the Office Action's allegations, Applicant has amended claims 26 and 50 to recite a "non-transitory computer readable medium" (emphasis added). Applicant notes that such a recitation is permissible, as discussed in the *Interim Examination Instructions for Evaluating Subject Matter Eligibility under 35 U.S.C. § 101* (Aug. 2009). For example,

> a claim to a non-transitory, tangible computer readable storage medium *per se* that possesses structural limitations under the broadest reasonable interpretation standard to qualify as a manufacture would be patent-eligible subject matter. Adding additional claim limitations to the medium, such as executable instructions or stored data, to such a statutory eligible claim would

> not render the medium non-statutory, so long as the claim as a whole has a real world use and the medium does not cover substantially all practical uses of a judicial exception. The claim as a whole remains a tangible embodiment and qualifies as a manufacture.

Interim Instructions at 4.

Applicants therefore respectfully request withdrawal of the 35 U.S.C. § 101 rejection.

C. Claim rejections under 35 U.S.C. § 102(a)

Applicant requests reconsideration and withdrawal of the rejection of claims 26-28, 30-32, 35-40, 42-44, and 47-50 under 35 U.S.C. § 102(a) as being anticipated by Lahtinen. In order to establish anticipation under 35 U.S.C. § 102, the Federal Circuit has held that "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Furthermore, "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1126, 1236, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989). *See also* M.P.E.P. § 2131. Here, Lahtinen does not disclose each and every element of at least independent claim 38.

Independent Claims 26 and 38

Lahtinen, at least, does not disclose an intrusion detection system, for detecting unauthorised use of a network, comprising at least one computer; and a non-transitory computer readable medium encoded with a computer program product which includes:

> instructions for ... capturing data being transmitted on said network,
>
> instructions for ... comparing the captured data with attack signatures for generating an event when a match between the captured data and at least one attack signature is found, and

> instructions for a response analysis engine triggered by said event, for comparing with response signatures response data being transmitted on said network as a response to said data matched with said at least one attack signature,

as, for example, recited in amended claim 26 (emphases added).

In its rejection of claim 26, on pages 5-6, and in its Response to Arguments, on pages 2-3, the Final Office Action asserted that the above underlined features are disclosed by Lahtinen in Fig 2, Fig. 6 blocks 612, 614, and 616, and paragraphs [0028]-[0034] and [0057]-[0060]. Applicant respectfully disagrees. Lahtinen is directed to "monitoring of the flow of a data stream traveling between a client and a server system." Lahtinen at page 1. The cited paragraphs [0028]-[0034], corresponding to Fig. 2, describe that a data stream from a client is inspected by an inspection block 206. If the data stream is suspected to be an attack attempt, the data stream is "forwarded to an event analysis and reporting block 240." Lahtinen at [0031]. Further, the cited paragraphs [0057]-[0060], corresponding to Fig. 6, describe a similar process for handling a request sent from a client (i.e., a user agent shown in Fig. 3) to a server. *See Id.* at [0057]. The request is analyzed by inspection block 206 and, if the request includes anomalies, e.g., invalid parameters, an event classification step 616 is invoked and, if necessary, an alert is generated in step 618. *See Id.* at [0060], [0065], and [0067].

Contrary to the assertion by the Final Office Action on pages 3 and 6, such event classification 616 does not trigger "comparing with response signatures ... response data being transmitted ... as a response to said data matched with said at least one attack signature," as recited in claim 38. Lahtinen discloses that, in some cases, once an alert is generated, "the request is blocked, i.e. it is not forwarded to the web server." *Id.* at [0060]. Therefore, once the suspicious request is blocked, there will be no response to that request. Further, in some cases Lahtinen discloses that the event classification classifies the request as not harmful and thus

allows the request to be forwarded. *Id.* at [0068]. However, Lahtinen still does not disclose, and the Final Office Action failed to specifically point out where Lahtinen does disclose, that as a result of event classification 616, a comparison in the manner recited in claim 38, is performed on a response to the request.

Independent claim 38, although differing in its scope from claim 26, recites features similar to the above features of claim 26. Therefore, for at least the above reasons, Lahtinen does not anticipate claim 38.

Dependent Claims 27, 28, 30-32, 35-37, 39, 40, 42-44, and 47-50

Lahtinen does not anticipate claims 27, 28, 30-32, 35-37, 39, 40, 42-44, and 47-50, at least by virtue of their dependence, either directly or indirectly, from claims 26 and 38.

Moreover, claims 30 and 42 recite that the alarm is generated "when said response data indicates that a new network connection has been established." In its rejection of claim 30 on page 7, the Final Office Action asserted that paragraph [0044] of Lahtinen discloses these recited features. Applicant respectfully disagrees. The cited paragraph merely describes a process of analyzing a request-response pair as explained above, and it does not describe or suggest that first an event is triggered in the manner recited in claim 38, and then, triggered by the event, a response data is analyzed and it is determined that a new network connection has been established, as required by claims 30 and 42. Lahtinen does not disclose these features as recited in claims 30 and 42 and the Final Office Action failed to clearly point out where it does.

Moreover, claims 31 and 43 recite that "response signatures are arranged in two categories, response signatures identifying illicit traffic, and response signatures identifying legitimate traffic." In its rejection of claim 31 on page 7, the Final Office Action asserted that Fig. 7 and paragraph [0032] of Lahtinen disclose these recited features. Applicant respectfully

disagrees. In Lahtinen, Fig. 7 and paragraph [0032] describe available states for a client and possible legitimate/valid requests that may come from the client. These excerpts at most disclose identifying the request from client as being or not being legitimate. Nowhere does Lahtinen disclose that first an event is triggered in the manner recited in claim 38, and then, triggered by the event, a response data is analyzed and "response signatures are arranged in two categories ... [of] illicit traffic, and ... legitimate traffic," as recited in claims 31 and 43 (emphasis added). Lahtinen does not disclose these features as recited in claims 31 and 43 and the Final Office Action failed to point out where it does.

Further, claims 35 and 47 recite "a time-out system, triggered by said event, for starting a probing task." In its rejection of claim 35 on page 7, the Final Office Action asserted that paragraph [0068] of Lahtinen discloses these recited features. Applicant respectfully disagrees. In Lahtinen, paragraph [0068] merely describes "FIG. 7 [which] shows how the table of available states is initialized when a new client and/or host is observed for the first time." Paragraph [0068] does not disclose that first an event is triggered in the manner recited in claims 26 or 38, and then, triggered by the event, "a time-out system [is provided] ... for starting a probing task," as, for example, recited in claim 47. Lahtinen does not disclose these features and the Final Office Action failed to point out where it does.

Additionally, claim 48, which depends from claim 47 above, recites that the method further comprises

> verifying if any data has been detected on said network as a response to said data matched with said at least one attack signature, and, if such condition is verified: generating the alarm in case only response signatures indicating legitimate traffic have been used; or
>
> ending said probing task in case only response signatures indicating illicit traffic or both response signatures indicating legitimate traffic and illicit traffic have been used.

In its rejection of claim 36 on page 8, the Final Office Action cited excerpts which disclose generating an alarm, limiting false alarms, and Fig. 1B and paragraph [0009] of Lahtinen. The Final Office Action, however, failed to point out any section of Lahtinen which specifically disclose the above recited features of claim 48, or similar features recited in claim 36, once a probing task is started in the manner recited in claim 47.

Moreover, claim 49, which depends from claim 48 above, recites that "if such condition [as recited in claim 48] is not verified, said probing task attempts to perform a connection to a suspected attacked computer, for generating the alarm if such attempt is successful, or for ending the probing task if such attempt is unsuccessful." In its rejection of claim 37 on page 8, the Final Office Action asserted that paragraph [0009] and Fig. 1B of Lahtinen disclose features similar to the above features of claim 49. Applicant respectfully disagrees. In the cited excerpts, or any other section, Lahtinen does not disclose, and the Final Office Action failed to point out specifically where it does, that once a probing tasks is started in the manner recited in claim 47, the probing task makes an attempt as recited in claims 37 and 49 and generates an alarm if the attempt is successful.

Accordingly, Applicant respectfully requests withdrawal of the 35 U.S.C. § 102(a) rejection.

D. Claim rejections under 35 U.S.C. § 103(a)

Applicant requests reconsideration and withdrawal of the remaining rejections of claims 29, 33, 34, 41, 45, and 46 under 35 U.S.C. § 103(a) as being unpatentable over Lahtinen in view of one or more of Yadav and Maher.

The Final Office Action has not properly resolved the *Graham* factual inquiries, the proper resolution of which is the requirement for establishing a framework for an objective

obviousness analysis. *See* M.P.E.P. § 2141(II), citing to *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), as reiterated by the U.S. Supreme Court in *KSR International Co. v. Teleflex Inc.*, 550 U.S. 398, 82 USPQ2d 1385 (2007). In particular, the Final Office Action has not properly determined the scope and content of the prior art, and has not properly ascertained the differences between the claimed invention and the prior art.

Applicant has previously established herein that Lahtinen does not teach or suggest each and every element of independent claims 26 and 38. The Final Office Action's application of Lahtinen alone or in combination with one or more of Yadav and Maher against the dependent claims does not cure the deficiencies of Lahtinen as to independent claims 26 and 38. The Final Office Action's allegations as to Lahtinen and the secondary references with regard to the dependent claims does not address the failure of Lahtinen to teach or suggest each and every element of claim 38, as explained in the previous section.

Specifically, on pages 10-11, the Final Office Action rejected claims 29 and 41 as being unpatentable over Lahtinen in view of Yadav. Further, on pages 11-12, the Final Office Action rejected claims 33, 34, 45, and 46, as being unpatentable over Lahtinen in view of Maher. In each rejection, the Final Office Action relied on Lahtinen to disclose all features of claims 26 and 38 from one of which the rejected claim depends, and further cited Yadav or Maher for the disclosure of additional features recited in the rejected claim. Yadav discloses an integrated network intrusion detection system which performs intrusion analysis on packets blocked by a firewall. *See* Yadav at Abstract. Maher, on the other hand, discloses a "content processor ... that is able to scan the contents of entire data packets including header and payload information." Maher at Abstract. Regardless of whether Yadav and Maher disclose the features for which the Final Office Action relied on them as to the dependent claims, which Applicant does not

concede, Yadav and Maher do not cure the deficiencies of Lahtinen, because they do not teach or suggest those features of claims 26 and 38 which are missing from Lahtinen, as discussed above.

Dependent claims 29, 33, 34, 41, 45, and 46 are therefore nonobvious and should be allowable at least by virtue of their dependence from base claims 26 and 38. Applicant therefore requests withdrawal of the remaining 35 U.S.C. § 103(a) rejections.

IV. Conclusion

Applicant respectfully requests reconsideration of this application and withdrawal of the rejection. Pending claims 26-50 are in condition for allowance, and Applicant requests a favorable action.

The Final Office Action contains statements characterizing the related art and the claims. Regardless of whether any such statements are specifically identified herein, Applicant declines to automatically subscribe to any such statements in the Final Office Action.

If there are any remaining issues or misunderstandings, Applicant requests that the Examiner telephone the undersigned representative to discuss them.

Please grant any extensions of time required to enter this response and charge any additional required fees to Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: April 28, 2010

By: 
Reza Sadr, Ph.D.
Reg. No. 63,292

/direct telephone: (617) 452-1563/